

**UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF OKLAHOMA**

STEVE M. GOLDSMITH,

Plaintiff,

V.

**UNITED STATES GOVERNMENT d/b/a
DVA and DR. JANET K. CATER, Ph.D,
CRC,**

Defendants.

Case No. 20-CV-0543-CVE-CDL

OPINION AND ORDER

Now before the Court is the Federal Defendants’ Motion to Dismiss (Dkt. # 7). Defendants argue that plaintiff has failed to state a claim under the Privacy Act, 5 U.S.C. § 552a (Privacy Act), the Health Insurance Portability and Accountability Act (HIPAA), or Oklahoma law for an alleged disclosure of his confidential information. Dkt. # 7. Plaintiff responds that Janet K. Cater, Ph. D., violated his rights under state and federal law by sending him an unencrypted e-mail containing his social security number, because this potentially exposed his confidential information to the “world wide net.” Dkt. # 14, at 2.

On October 26, 2020, plaintiff filed a pro se complaint alleging that Dr. Cater sent him an unencrypted e-mail, and there was an attachment to the e-mail that contained his social security number. Dkt. # 2, at 2. Plaintiff alleges that the e-mail included his full social security number in violation of regulations promulgated by the Department of Veterans Affairs (DVA), and he asked a privacy officer, David Eaton, to “sign [him] up for a security freeze.” Id. Eaton allegedly responded the government’s data was not compromised and there was not need to put a security freeze on plaintiff’s account. Id. Plaintiff claims that he has to “put a freeze on my credit report

every year and when I apply for any type of credit I have to undo the freeze and re-do the freeze every time.” Id. Plaintiff asserts claims under the Privacy Act and HIPAA, and he may also be attempting to bring a tort claim against the United States under the Federal Tort Claims Act, 28 U.S.C. § 1346(b) (FTCA).

Defendants have filed a motion to dismiss (Dkt. # 7) arguing that plaintiff has failed to state a claim upon which relief can be granted. In considering a motion to dismiss under Fed. R. Civ. P. 12(b)(6), a court must determine whether the claimant has stated a claim upon which relief may be granted. A motion to dismiss is properly granted when a complaint provides no “more than labels and conclusions, and a formulaic recitation of the elements of a cause of action.” Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 555 (2007). A complaint must contain enough “facts to state a claim to relief that is plausible on its face” and the factual allegations “must be enough to raise a right to relief above the speculative level.” Id. (citations omitted). “Once a claim has been stated adequately, it may be supported by showing any set of facts consistent with the allegations in the complaint.” Id. at 562. Although decided within an antitrust context, Twombly “expounded the pleading standard for all civil actions.” Ashcroft v. Iqbal, 556 U.S. 662, 683 (2009). For the purpose of making the dismissal determination, a court must accept all the well-pleaded allegations of the complaint as true, even if doubtful in fact, and must construe the allegations in the light most favorable to a claimant. Twombly, 550 U.S. at 555; Alvarado v. KOB-TV, L.L.C., 493 F.3d 1210, 1215 (10th Cir. 2007); Moffett v. Halliburton Energy Servs., Inc., 291 F.3d 1227, 1231 (10th Cir. 2002). However, a court need not accept as true those allegations that are conclusory in nature. Erikson v. Pawnee Cnty. Bd. of Cnty. Comm’rs, 263 F.3d 1151, 1154-55 (10th Cir. 2001). “[C]onclusory allegations without

supporting factual averments are insufficient to state a claim upon which relief can be based.” Hall v. Bellmon, 935 F.2d 1106, 1109-10 (10th Cir. 1991).

Defendants argue that plaintiff has not alleged that there was an improper disclosure of his personal information or that he was adversely affected by the sending of an unencrypted e-mail, and plaintiff’s Privacy Act claim should be dismissed. The Privacy Act states that “[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.” 5 U.S.C. § 552a(g)(1)(D). The Tenth Circuit has determined that a Privacy Act claim has four elements: “(1) the information is a record within a system of records, (2) the agency disclosed the information, (3) the disclosure adversely affected the plaintiff, and (4) the disclosure was willful or intentional.” Wilkerson v. Shinseki, 606 F.3d 1256, 1268 (10th Cir. 2010). The term “disclosure” is not defined in the Privacy Act, but the Tenth Circuit has interpreted “disclosure” to mean that a document or record was shared with “someone other than the data subject or the data subject’s authorized representative.” Id. In this case, plaintiff alleges that Dr. Cater sent him an unencrypted e-mail containing his social security number, and there was no disclosure of plaintiff’s personal information to a third party. Plaintiff alleges that his personal information was disclosed to the “world wide net,” because the e-mail he received was not encrypted. This argument is based on speculation that a third-party could unlawfully gain access to plaintiff’s e-mail, and this does not support an inference that Dr. Cater made an improper disclosure under the Privacy Act. Plaintiff’s complaint does not state a claim under the Privacy Act.

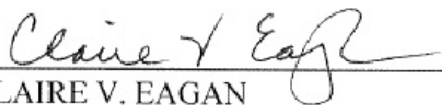
Defendants argue that HIPAA and regulations promulgated pursuant to HIPAA do not provide a private right of action for alleged disclosures of confidential information. The Tenth Circuit has found that HIPAA does not “create a private right of action for alleged disclosures of confidential medical information.” Wilkerson, 606 F. 3d at 1267 n.4. Plaintiff cites 45 C.F.R. §§ 164.502(b) and 164.514, which prevent a “covered entity or business associate” from disclosing the protected health care information of an individual. Section 164.502(b) requires that a covered entity “make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. 45 C.F.R. § 164.502(b). However, this regulation does not apply to disclosures made “[t]o the individual,” and the alleged disclosure in this case was made when Dr. Cater sent an e-mail to plaintiff. Section 164.514(d) provides guidance for covered entities for determining whether certain information is protected under HIPAA and for making the minimum necessary disclosure of confidential information, but there is nothing in the regulation suggesting that a private right of action exists pursuant to the regulation. 45 C.F.R. § 164.514(d). The Court finds that neither HIPAA nor the regulations cited by plaintiff create a private right of action, and plaintiff’s HIPAA claim should be dismissed.

Plaintiff could be attempting to assert tort claims against defendants, and defendants note that plaintiff did submit a notice of tort claim prior to filing this case. See Dkt. # 7-1. The notice of tort claim states that Dr. Cater “exposed [plaintiff’s] Social Security number to the world wide net” by sending plaintiff an unencrypted e-mail. Id. at 3. Defendants infer that the notice of tort claim asserts a claim against them for invasion of privacy. Dkt. # 7, at 8. Plaintiff also claims that Dr. Cater failed to comply with the DVA handbook, and he could be asserting a negligence claim against defendants. Id. at 3-4. The Court finds that the allegations of plaintiff’s complaint (Dkt. # 2) and

the notice of tort claim fail to state a colorable tort claim against defendants. Under Oklahoma law, an invasion of privacy claim based on an unauthorized disclosure of private information must be based on a public disclosure of information and the disclosure must have been highly offensive to a reasonable person. Thomas v. City of Bartlesville, Oklahoma, 2011 WL 5119518, *3-4 (N.D. Okla. Oct. 28, 2011). In this case, there was no public disclosure of plaintiff's personal information, and plaintiff's tort claims are based on his speculation that third-parties could steal his social security number from an unencrypted e-mail that was sent to his e-mail account. Plaintiff's fear that his personal information could be stolen from his e-mail account does not give rise to an invasion of privacy claim. This also does not show that he suffered an injury for the purpose of a negligence claim. The elements of a negligence claim under Oklahoma law are "(1) the existence of a duty on part of defendant to protect plaintiff from injury; (2) a violation of that duty; and (3) injury proximately resulting therefrom." Brigance v. Velvet Dove Restaurant, Inc., 725 P.2d 300, 302 (Okla. 1986). Plaintiff has not alleged any facts suggesting that he has actually suffered an injury caused by defendants' conduct, and his allegation concerning a risk of injury in the future are wholly speculative. Finally, the Court finds that the DVA handbook does not create any obligations that are enforceable by a federal court, and alleged violations of the handbook do not give rise to a claim for money damages. Nails v. Slusher, 2015 WL 12860496, *3 (D. Kan. May 20, 2015).

IT IS THEREFORE ORDERED that the Federal Defendants' Motion to Dismiss (Dkt. # 7) is **granted**. A separate judgment of dismissal is entered herewith.

DATED this 4th day of August, 2021.


 CLAIRE V. EAGAN
 UNITED STATES DISTRICT JUDGE